Environmental Management Consolidated Business Center (EMCBC)

Subject: Cyber Security Master Policy

Policy Statement APPROVED: _Signature on File_____________
EMCBC Director
ISSUED BY: OFFICE OF INFORMATION RESOURCE MANAGEMENT

1.0 PURPOSE

Title III (§301) of the E-Government Act (Public Law 107-347), passed November 15, 2002, is known as the Federal Information Security Management Act (FISMA) of 2002. This act requires that all federal agencies (U.S. civilian departments, agencies, and their contractors) develop and implement an agency-wide information security program to safeguard the Information Technology (IT) assets and data of the respective agency.

In 2004 and 2005, the National Institute of Standards and Technology (NIST) released a series of new guidance documents that restructured the certification and accreditation process (NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*) by requiring demonstrations of the processes and controls used to ensure a defense-in-depth computer security architecture. NIST is specific in its requirements and stipulates that the information security program must include documentation and reports that clearly describe the following:

- Periodic risk assessments
- Information security policies and procedures
- An assessment of threats, including their likelihood and impact
- Policies and procedures for detecting security vulnerabilities
- Evaluation and periodic testing of how well security policies are working
- An inventory of software and hardware assets
- Security awareness training and expected rules of behavior for end-users
- An evaluation of the technical, management, and operational security controls
- Procedures for reporting and responding to security incidents
- A process for addressing any deficiencies reported
- Contingency plans to ensure continuity of operations during a disaster

Federal Information Processing Standard (FIPS) 199 offers a standardized methodology to assess the risks to the confidentiality, integrity, and availability (CIA) of unclassified systems. NIST SP 800-60 provides guidance for mapping types of information systems to recommended baseline CIA security categories. NIST SP 800-53 sets out the baseline management, operational, and technical controls that systems must incorporate into a system to minimally ensure the security of low, moderate, and high risk systems. This set of documents is reflected in FIPS 200. FISMA requires that Federal agencies report their cyber security programs in accordance with this new guidance, which highlights all laws and regulations on Cyber Security.

This document outlines the requirements of NIST 800-53 for cyber security policies. It also includes a policy statement describing the implementation of a Software Quality Assurance program in accordance with the EMCBC Quality Assurance Implementation Plan, PL-414-04 (QIP). It is not intended to be a substitute for the DOE Office of the Under Secretary of Energy's Environmental Management Program Cyber Security Plan (Energy PCSP), but rather is a policy statement of requirement for security controls.

2.0 SCOPE

This policy applies to all unclassified cyber systems and networks which are part of the Environmental Management Consolidated Business Center (EMCBC) cyber systems accreditation boundaries and associated enclaves. This policy is intended to identify and outline the computer security policy statements implemented or to be implemented in consonance with the referenced documents below. It specifically identifies the management, operational, and technical controls that must be incorporated into the EMCBC accreditation boundary to ensure the security of low and moderate risk systems. This policy specifies the responsible EMCBC department(s) and/or responsible official for the implementation of the control policies.

3.0 APPLICABILITY

This EMCBC policy applies to all entities, Federal or contractor, that collect, create, process, transmit, store, and disseminate information for the EMCBC organization.

This policy applies to any information system that collects, creates, processes, transmits, stores, and disseminates unclassified DOE information. This policy applies to all points in the information system life cycle, including the development of new information systems, the incorporation of information systems into an infrastructure, the incorporation of information systems outside the infrastructure, the development of prototype information systems, the reconfiguration or upgrade of existing systems, and legacy systems. In this document, the term(s) "information system" or "system" are used to mean any information systems and/or networks that are used to collect, create, process, transmit, store, or disseminate data owned by, for, or on behalf of EMCBC or DOE.

4.0 REQUIREMENTS AND REFRENCES

4.1 Requirements:

Requirements are performance based approaches and must be used to evaluate and verify the effectiveness of cyber security measures, as well as to identify areas requiring improvement and to validate implemented improvements. Protection measures for all EMCBC information systems must conform to the protection measures described in the Energy PCSP, and the information System Security Plans (SSP). As a minimum, the protection afforded to the information and information system, on which it resides, is based on a risk-based graded protection approach as defined by the Energy PCSP. Protection measures may be strengthened based on an assessment of unique local threat(s) or the local evaluation of Consequence of Loss.

All information on an EMCBC information system must be considered when determining the system's protection measures.

4.2 References:

4.2.1 44 USC Chapter 35, Subchapter III, Federal Information Security Management Act (FISMA);

4.2.2 Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors;

4.2.3 NIST SP 800-53 - Recommended Security Controls for Federal Information Systems;

4.2.4 NIST SP 800-53A – Guide for Assessing the Security Controls in the Federal Information Systems;

4.2.5 NIST SP 800-26 – Security Self-Assessment Guide for Information Technology Systems;

4.2.6 FIPS PUB 199 – Standards for Security Categorization of Federal Information and Information Systems;

4.2.7 FIPS PUB 200 – Minimum Security Requirements for Federal Information and Information Systems;

4.2.8 NIST SP 800-30 - Risk Management Guide IT Systems;

4.2.9 NIST SP 800-37 – Security Certification and Accreditation;

4.2.10 NIST SP 800-27A Engineering Principles for Information Technology Security;

4.2.11 DOE Order 205.1B – Department of Energy Cyber Security Program;

4.2.12 Office of Management and Budget (OMB) Circular No. A-130, Management of Federal Information Resources;

4.2.13 DOE Office of the Under Secretary of Energy Program Cyber Security Plan (Energy PCSP);

4.2.14 PL-240-08, Cyber Security - System Security Plan for General Support System;

4.2.15 PL-414-01 – EMCBC Quality Policy

4.2.16 PL-414-04 – EMCBC QA Implementation Plan (QIP)

4.2.17 DOE Memo dated 8/23/11, from Jack Craig to John Muskoff, Information System Security Manager, subject: EMCBC Authority to Operate

5.0 DEFINITIONS

The following are terms and definitions used in this policy that are not found in National Security Telecommunications and Information Systems Security (NSTISSC) 4009, National Information Systems Security (INFOSEC) Glossary, dated 5 June 1992, unless otherwise noted.

5.1 Access Approval - Access to information is authorized in writing with justification. Documented approval by a data or system owner to allow user access to information.

5.2 Accreditation (INFOSEC Glossary) - Formal declaration by the Authorizing Official (AO) that an information system is accredited to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

5.3 Accreditation Boundary - The conceptual limit of an information system that extends to all directly and indirectly connected users who receive output from the system without a reliable human review by an appropriately authorized or cleared authority.

5.4 Architecture - The configuration of any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; includes computers, ancillary equipment and services, including support services and related resources.

5.5 Assurance (INFOSEC Glossary) - Measure of confidence that the security features, practices, procedures and architecture of an information system accurately mediate and enforce the security policy.

5.6 Authority to Operate (ATO) – Formal documentation from a senior organizational official that verifies the system meets the requirements as stated in the System Security Plan and authorizes (accredits) the information system for processing.

5.7 Authorizing Official (AO) - Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority.

5.8 Certification and Accreditation (C&A) – The process of formal assessment, testing (certification), and acceptance (accreditation) of system security controls that protect information systems and data stored in and processed by those systems. This process encompasses the system's life cycle and ensures that the risk of operating a system is recognized, evaluated, and accepted.

5.9 Confidentiality (INFOSEC Glossary) - A security objective that seeks to assure that information is not disclosed to unauthorized persons, processes, or devices. (NSTISSI No. 4009: Assurance that information is not disclosed to unauthorized persons, processes, or devices.)

5.10 Consequence of Loss (CoL) – Methodology used to determine the consequence, if any, that might occur if the asset was lost, using the impact factors.

5.11 Content Manager - The person acting on behalf of the data owner for the generation, management, and destruction of data and to ensure the review of information sensitivity and classification.

5.12 Content Owner - The person responsible for having information reviewed for sensitivity and classification. This person is responsible for its generation, management, and destruction.

5.13 Defense-in-depth - Represents the use of multiple computer security techniques to help mitigate the risk of one component of the defense being compromised or circumvented. An example could be anti-virus software installed on individual workstations when there is already virus protection on the firewalls and servers within the same environment. Different security products from multiple vendors may be on different vectors within the network, helping prevent a shortfall in any one defense leading to a wider failure.

5.14 General Support System - An interconnected set of information resources under the same direct management control that share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that support a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization. [From Office of Management and Budget (OMB) Circular A-130, Appendix III.]

5.15 Information Integrity -The preservation of unaltered states as information is transferred through the system and between components.

5.16 Information System (INFOSEC Glossary) - The infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. Any telecommunication or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware. [Office of Management and Budget, Circular A-130, Nov. 30, 2000: A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.]

5.17 Information System Security Manager (ISSM) - The official responsible for performing the comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meet a set of specified security requirements, and ensuring the approved security configuration is maintained.

5.18 Information System Security Officer (ISSO) (INFOSEC Glossary) - Person responsible to the system owner and AO for ensuring the security of an information system throughout its life cycle, from design through disposal. Synonymous with system security officer.

5.19 Information Technology (IT) - The hardware, firmware, and software used as part of the information system to perform information functions. This definition includes computers, telecommunications, automated information systems, and automatic data processing equipment. IT includes any assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an agency.

5.20 Integrity - Guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542] A loss of integrity is the unauthorized modification or destruction of information.

5.21 Legacy Information System - An operational information system that existed prior to the implementation of the C&A process.

5.22 Major Application - A major application is an application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. [From Appendix III, OMB A-130]

5.23 Mission - The assigned duties to be performed by an information system.

5.24 Perimeter - All components of an information system that are to be accredited as one entity.

5.25 Personally Owned - An item that is owned by an individual and is intended solely for his/her personal use.

5.26 Portable Computing Device - Any portable device that provides the capability to collect, create, process, transmit, store, and disseminate information. They include (but are not limited to) Personal Digital Assistants (PDAs), palm tops, hand-held or portable computers and workstations, non-web-enabled cell phones, web based enhanced cell phones, two-way pagers, and wireless e-mail devices.

5.27 Privileged User - A user with access to control, monitoring, or administration functions of the information system (e.g., system administrator, system security officer, maintainers, system programmers, etc.). NOTE: It is often convenient to refer to a user who is NOT a privileged user as a power user.

5.28 Protection Profile - An implementation- independent set of security requirements for a category of information systems that meet specific protection measures for specific information groups.

5.29 Risk Assessment (INFOSEC Glossary) - Process of analyzing threats to and vulnerabilities of an information system and the potential impact the loss of information or capabilities of a system would have on national security. The resulting analysis is a basis for identifying appropriate and cost-effective countermeasures.

5.30 Risk Management (INFOSEC Glossary) - The process concerned with the identification, measurement, control, and minimization of security risks in information systems to a level commensurate with the value of the assets protected.

5.31 Security - Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.

5.32 Security Documentation - All documents which describe the security requirements, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system or major application (or update to either) meets the protection requirements.

5.33 Site Manager - The person responsible for management of all activities at an element.

5.34 System - The set of interrelated components consisting of mission, environment, and architecture as a whole.

5.35 System Owner - The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system.

5.36 System Security Plan (SSP) - Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

5.37 User (INFOSEC Glossary) - An individual who can receive information from, input information to, or modify information on an information system without an independent human review.

5.38 Vulnerability Assessment (INFOSEC Glossary) - Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

6.0 RESPONSIBILITIES

EMCBC's organizational structure is listed below and the responsibilities are identified to implement the computer security controls.

6.1 Authorizing Official (AO)

The AO is a federal senior management official with budget and oversight authorities within the organization who assumes the responsibility for an information system and is held accountable for ensuring the information system is operating at an acceptable level of risk. The role of the AO, with the requirements specified below, must be defined and applied to all systems, both classified and unclassified.

AOs assume full responsibility for the residual risk of an information system's operation. AOs are also responsible for ensuring that the level of risk does not reach an unacceptable level during operation and that risk is reassessed when a significant change occurs. The following are AO requirements:

- Possess a clearance to the highest classification level of the systems to be accredited;
- Receive training specific to the role within six months of appointment;
- Possess technical knowledge of the systems to be accredited in order to understand technical countermeasures or cyber threats;
- Hold a minimum of a DOE L Clearance (must be cleared to the level required to view threat information); and,
- Be a senior management official working directly for the Program, Site or Laboratory Manager.

If the AO is a senior management official working directly for a manager as above, that individual will also be a manager that has oversight of resources and funding for the IT assets to be accredited.

Through security accreditation, the AO assumes responsibility and is accountable for the risks associated with operating an information system. Additionally, the AO will be called upon to:

- Approve system security requirements, SSPs, and memorandums of agreement and/or memorandums of understanding;
- Authorize operation of the information system, issue an interim authorization to operate the information system under specific terms and conditions, or deny authorization to operate the information system (or if the system is already operational, halt operations) if unacceptable security risks exist;
- Provide cyber security incident coordination with law enforcement agencies, safeguards and security organizations, Office of Inspector General, and Office of

Intelligence and Counterintelligence for the operating units under his/her cognizance, in coordination with the Information Systems Security Manager (ISSM);

- Participate in ongoing Senior DOE Management cyber security training and awareness program; and
- Provide input on the adequacy of Restricted Data (RD) protection to the intelligence system AO based on reviews of certification and accreditation (C&A) results for National Security Systems that process intelligence information and RD, as applicable.

Due to the breadth of organizational responsibilities and significant demands on time, an AO may designate a representative who is empowered to make certain decisions with regard to the planning and resource of the C&A activities. All AO responsibilities may be delegated to the Authorizing Official Designated Representative (AODR), with the exception of the decision to authorize operation of information systems. The accreditation letter must be signed by the AO. Federal and contractor staffs are required to follow the cyber security guidelines issued by the AO.

6.2 Authorizing Official Designated Representative (AODR)

The AODR is a management official who is appointed in writing by the AO to carry out the day-to-day implementation of the duties tasked to the AO. The AODR is required to be a federal employee. An AODR must also be formally trained in AO responsibilities. Multiple AODRs may be designated for a site or office, if necessary.

The AODR is responsible for:

- Day-to-day implementation of duties tasked to the AO;
- Certifying to the AO that all requirements have been met and that the information systems in EMCBC accreditation boundary are ready for accreditation;
- Recommending policies, standards, procedures and guidelines be adopted in EMCBC accreditation boundary for AO signature;
- Reviewing current technology for more effective security practices;
- Securing funding for EMCBC cyber security program;
- Providing coordination and interface with other aspects of security;
- Overseeing training activities and security awareness;
- Developing publications and bulletins on a as needed basis;
- Performing independent validations and verification; and
- Performing and maintaining Computer Incident Advisory Capability (CIAC) and EM cyber security incidents are promptly and properly reported.

6.3 Program Office Cyber Security Program Manager (CSPM)

The CSPM must be a federal employee working in a program office that reports through the Under Secretary and knowledgeable in cyber security. The CSPM has cyber security responsibilities for any organization under his or her purview, including the following:

- Ensures the implementation of the applicable Energy PCSP;
- Serves as the primary point of contact for cyber security for EMCBC;
- Is cognizant of the AO and AODR for all systems, including their suitability for this role;
- Develops and reviews (at least annually) the applicable Energy PCSP (if applicable), and reviews SSPs;
- Reviews DOE Risk and Threat statements as they become available;
- Approves minimum information system configurations for sites;
- Ensures adequate cyber security training, education, and awareness is available, that employees receive training according to policy, and that training records are maintained;
- Evaluates incident reports and ensure that designated individuals are regularly monitoring sources (such as SANS [System Administration, Audit, Network, and Security] Institute) for new vulnerabilities;
- Monitors the Energy PCSP and SSP compliance through program reviews, budget reviews, self-assessments, management assessments, performance metrics analysis, and analysis of the results of peer reviews, vulnerability assessments, and independent oversight evaluation;
- Ensures the development and coordination of corrective actions plans in response to issues identified by the Office of the Chief Information Officer (OCIO), Office of the Inspector General (OIG), Office of Health, Safety and Security (HSS), peer reviews, and self-assessments; and,
- Evaluates system changes to determine if they are significant and require re-certification and advises the AO in this capacity.

6.4 Information System Security Manager (ISSM)

The Information System Security Manager (ISSM) is considered the lead security personnel at the field sites within any Program Office and has working knowledge of system functions, cyber security policies, and technical cyber security protection measures. This individual is responsible for conducting testing, as well as performing all “local” responsibilities designated by the field site. The ISSM is appointed in writing by the field site manager in conjunction with concurrence from the AO, or by the AO. The ISSM may serve as the Certification Agent (CA) in cases where duties are operationally separate. The ISSM is also responsible for maintaining the records related to C&A packages and Plan of Action & Milestones (POA&M). The ISSM responsibilities include the following:

- Establishes, documents, and monitors the operating unit’s cyber security program implementation and ensures operating unit compliance with departmental policy and the Energy PCSP.
- Ensures that plan of action and milestones (POA&Ms) are prepared and coordinated with other security disciplines, as necessary, for program or system level findings.
- Ensures that the organization plans, budgets, allocates, and spends adequate resources in support of cyber security.
- Oversees all operating unit information system security officers (ISSOs) to ensure

that they follow established information security policies and procedures.

- Ensures that users are trained on the information system's cyber security features, operation, and safeguards prior to being allowed access to the system.
- Ensures that personnel with cyber security responsibilities are trained on cyber security requirements, operations, safeguards, and incident handling procedures.
- In coordination with the operating unit's operations security (OPSEC) program, identifies and documents operating unit-specific threats to information systems and information.
- Ensures that the operating unit cyber security program is coordinated with other operating unit plans/programs to include: disaster recovery, site safeguards and security plan or site security plan, classified matter protection and control, physical security, personnel security, telecommunications security, TEMPEST, technical surveillance countermeasures, operations security, counterintelligence, and nuclear materials control and accountability.
- Ensures that the cognizant AO/AODR is notified when the information system is no longer needed or when changes occur that might affect the accreditation of the information system.
- Participates in DOE- and Senior DOE Management-sponsored cyber security training within six (6) months of his/her appointment.
- Ensures that an AO-approved overwrite method and a review process is used for sanitization and the review of the results of overwrites to verify that the method used completely overwrote all classified or sensitive information.
- Ensures that computer incident advisory capability alerts are analyzed, necessary corrective actions are accomplished, and status reported and that suspected cyber security incidents are investigated, analyzed, documented, and reported to the AO/AODR.
- Ensures that self-assessments are conducted.
- Ensures that each individual responsible for a major application within the operating unit is aware of and fulfills his/her cyber security duties.
- Evaluates system changes to determine whether they are significant and require re-certification and advises the AO in this capacity.
- Provides cyber security incident coordination with law enforcement agencies, safeguards and security organizations, Office of Inspector General, and Office of Intelligence and Counterintelligence for the operating units under his/her cognizance, in coordination with the AO.
-

6.5 Certification Agent (CA)

The functional role of CA must be fulfilled by an individual who has a working knowledge of system function, security policies, and technical security safeguards. To ensure the integrity of the certification assessment, the CA must be independent of system development and operations teams, as well as those individuals responsible for correcting security deficiencies identified during the certification. The independence of the CA ensures the AO receives the most objective information possible in order to make an informed, risk-based accreditation decision.

The Program Office CSPM or ISSM will oversee the CA. Each C&A system will have a CA designated as part of the SSP, which will also document the independence of the CA. The system owner cannot act as the CA for unclassified systems classified as moderate and high impact or for any national security system.

The CA is responsible for conducting a comprehensive assessment of the management, operational, and technical security controls in an information system. The CA must also provide the system owner with the level of effort and resource requirements for conducting the security testing and evaluation (ST&E) process. The purpose of the security assessment is to determine the extent to which controls exist, are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting the security requirements for the system. Once the security assessment is complete, the CA provides any recommended corrective actions in order to reduce or eliminate vulnerabilities in the information system to the AO.

6.6 Information Systems Security Officer (ISSO)

Information System Security Officer (ISSO) is a term used to identify the individual assigned the responsibility for ensuring that cyber security policies and practices are applied to an information system. The functional role of ISSO must be appointed in writing to an individual who has a working knowledge of system functions, cyber security policies, and technical cyber security protection measures. The ISSO must have the detailed knowledge and expertise required to manage the security aspects of the information system and is generally assigned responsibility for the day-to-day security operations of the system. The ISSO serves as the point of contact for inquiries related to C&A processes. The ISSO responsibilities include the following:

- Ensures the implementation of protection measures that are documented in SSP for each information system under ISSO jurisdiction;
- Ensures that users are granted access to information systems' resources based on the least privilege principle;
- Identifies unique threats to information systems and documents threats in the SSP;
- Documents any special protection requirements identified by the application owner, data owner, or data steward and ensures that these requirements are included within the protection measures implemented in the information system;
- Ensures each information system under ISSO jurisdiction is covered by a SSP;
- Maintains a copy of the SSP for each information system under ISSO jurisdiction;
- Ensures the implementation of site procedures;
- Ensures that the organization's cyber security manager is notified when an information system is no longer needed or when the changes occur that might affect the accreditation of the information system;
- Ensures that information access controls and cyber protection measures are implemented for each information system as described by its SSP;
- Ensures that users and systems administrators are properly trained in information system security by identifying cyber security training needs and the personnel who need to attend the cyber security training program;
- Conducts cyber security reviews and tests to ensure that the cyber security features

and controls are functioning and effective;

- Ensures the performance of a risk assessment to determine if additional countermeasures beyond those identified in the SSP are required and whether an identified unique local threat exists;
- Communicates individual incident reports to the ISSM;
- Ensures the implementation of all applicable protection measures for each information system;
- Ensures that unauthorized personnel are not granted use of, or access to, the information system;
- Ensures that all users have requisite security clearances, authorization, and need-to-know and are aware of their security responsibilities before granting access to the information system;
- Ensures that each information system user acknowledges, in writing, his/her responsibility (code of conduct) for the security of information systems and information;
- Maintains a record copy of the C&A package for each information system for which he/she is the ISSO;
- Participates in ISSM self-assessment and training programs; and,
- Provides written notification to the cognizant information owners prior to granting any foreign national access to the information system.

6.7 Content Owners/Managers

All Application/Data Owners assume the following roles and responsibilities, including:

- Determining and declaring the classification level of the information prior to the information being processed, stored, transferred, or accessed on EMCBC information systems;
- Determining and documenting the mission essentiality of the information for which he or she is custodian and informing the ISSO;
- Providing the ISSO and System Administrator with any special security requirements for the information to be processed on information system;
- Defining appropriate data sets in order to be processed, stored, transferred, or accessed on the appropriate information system;
- Determining if disaster recovery and contingency plans are needed for information systems which they are responsible;
- Identifying and documenting unique threats to information systems and reporting them to the ISSO and/or ISSM;
- Advising the ISSO of any special confidentiality, integrity, or availability protection requirements for the information; and,
- Ensuring that the information is processed only on a system that is approved at a level to protect the information.

6.8 System Administrator

The System Administrator is responsible for maintaining and operating the systems and networks within an organization. Duties include day-to-day support, and are often wide-ranging. The System Administrator can expect to be charged with installing, supporting, and maintaining computer systems, and planning for and responding to service outages and other problems. The System Administrator typically manages user accounts including the deletion, creation, and modification of user privileges. System Administrators must ensure timely removal of access rights for all departed employees, especially in cases of employee termination. All DOE System Administrators must sign and abide by *Privileged User Rules of Behavior* (RoB). Additionally, System Administrators must receive annual training specific to their role.

The System Administrator is responsible for complying with the following program requirements:

- Ensuring authorized personnel comply with computer security requirements;
- Ensuring that the end user has read and signed the Rules of Behavior User Agreements before access is granted;
- Ensuring that all information systems are properly patched in a timely manner;
- Ensuring that information processed is properly protected;
- Ensuring that general end users are properly trained on computer security requirements;
- Ensuring that disaster recovery and contingency plans defined by Data Owner and Line Managers for EMCBC information systems are being complied;
- Ensuring that information systems are monitored and periodically evaluated to prevent or detect computer security incidents including instances of waste, fraud, or abuse;
- Reviewing SSPs and TIDs for compliance prior to submitting them to the ISSO; and,
- Reporting all suspicious or abnormal activities to ISSO and/or ISSM within 30 minutes of event or incident finding.

6.9 Line Managers

Line Managers are responsible for complying with the following program requirements:

- Concurring with the determination of critical resources within their organization, if they are found as mission essential, and information systems and associated networks, whether they are found as mission essential or non-mission essential;
- Notifying the system administrator and ISSO when a user should be removed from the system (i.e., in the case of termination, transfer, etc.);
- Ensuring that their employees are aware of site computer security procedures and the consequences of not adhering to those procedures;
- Ensuring that authorized personnel are appropriately screened and cleared to a level commensurate with the sensitivity of the data to be accessed or handled and the risk and magnitude of loss or harm that could be caused by the individual;
- Determining if disaster recovery and contingency plans are needed for information systems for which they are responsible;

- Making, documenting, and signing a decision concerning the need for a disaster recovery and contingency plan for the systems within EMCBC accreditation boundary;
- Ensuring that disaster recovery and contingency plans are developed when applicable, and that they are reasonable and sufficient; and
- Supporting the ISSM and ISSO personnel in the investigation of computer security incidents and in the implementation of corrective actions.

6.10 General Users/End Users

A general user, or end user, refers to any user who has not been granted system administrator, network administrator, or super-user status or root access, and does not have authority to change the cyber security configuration of an information system. The general user roles and responsibilities apply to all cyber assets and include the following:

- Complies with the requirements of the Energy PCSP and SSPs, as applicable;
- Is aware of, and knowledgeable about, responsibilities in regard to information systems security;
- Ensures that any authentication mechanisms issued for the control of access to information or information systems are not shared and are protected at the same level of protection applied to the information to which it permits access;
- Reports any compromise or suspected compromise of an authenticator to the appropriate ISSO;
- Is responsible and accountable for individual actions on an information system;
- Acknowledges, in writing, responsibilities for protecting information systems and classified information identified in the Annual Cyber Security Awareness Training and on IP-240-01-F1, Rules of Behavior for EMCBC Computer Systems;
- Participates in training on the information system's prescribed security restrictions and safeguards before initial access to a system;
- Reports all security incidents and potential threats and vulnerabilities involving the information system to the appropriate ISSO;
- Ensures that system media and system output are properly classified, marked, controlled, and stored;
- Protects terminals from unauthorized access as described in the information system security plan;
- Informs the ISSO when access to a particular information system is no longer required (e.g., completion of a project, transfer, retirement, resignation);
- Signs and abides by IP-240-01-F1, Rules of Behavior for EMCBC Computer Systems;
- Obtains classification review by their Line Manager;
- Provides protection for all media assigned to them at all times to at least the level commensurate with the sensitivity or classification level and category of the information stored on the media;
- Ensures that all media is properly sanitized and destroyed when it is no longer needed; and

- Remains alert for any adverse event that could have an impact on the Department of Energy and EMCBC.

7.0 GENERAL INFORMATION

This policy defines the roles and responsibilities used for performing the core cyber security functions for all EMCBC unclassified accreditation boundaries. The implementation of stated policy is the responsibility of both federal employees and associated support service contractors, whose individual understanding of and involvement in the EMCBC cyber security program is critical to its success.

8.0 RECORDS MAINTENANCE

8.1 Records generated as a result of implementing this policy are identified as follows:

8.1.1 IP-251-01-F1, EMCBC Record of Revision (Attachment E)

9.0 FORMS USED

9.1 Privileged User Rules of Behavior (RoB)

9.2 Rules of Behavior for EMCBC Information Systems

10.0 ATTACHMENTS

Computer Master Security Policy Statements Attached:

Attachment Number	Class	Policy Statement	Identifier
10.1	Management	**Risk Assessment**	RA
10.2	Management	**Security Planning**	PL
10.3	Management	**System and Services Acquisition**	SA
10.4	Management	**Certification, Accreditation, and Security Assessment**	CA
10.5	Operational	**Personnel Security**	PS
10.6	Operational	**Physical and Environmental Protection**	PE
10.7	Operational	**Contingency Planning**	CP
10.8	Operational	**Configuration Management**	CM
10.9	Operational	**Maintenance**	MA
10.10	Operational	**System and Information Integrity**	SI
10.11	Operational	**Media Protection**	MP
10.12	Operational	**Incident Response**	IR
10.13	Operational	**Awareness and Training**	AT
10.14	Technical	**Identification and Authentication**	IA
10.15	Technical	**Access Control**	AC
10.16	Technical	**Audit and Accountability**	AU
10.17	Technical	**System and Communications Protection**	SC
10.18	QIP	**Software Quality Assurance**	SQ

ATTACHMENT 10.1

Risk Assessment (RA) Policy Statement

Purpose:

This Risk Assessment Policy Statement has been established to ensure that cost effective mitigation strategies are applied to the EMCBC environment to implement a defense posture commensurate with the risk of compromise or destruction of the information being developed, transmitted, or stored. These strategies must ensure that the missions of the EMCBC are protected, not just its information assets.

Security controls will be assessed for effectiveness and applicability to the EMCBC environment and will be placed at the most critical or beneficial points. Controls shall be selected to cost effectively maximize the reduction in risk. Risk assessment is a continuous process, incorporating both a formal risk analysis and ongoing reassessment. The methods outlined in NIST SP 800-30 will be used for risk analysis. Mitigation strategies will be based on the degree of risk as well as the cost-effectiveness of the strategy and implemented through a POA&M to correct / reduce the vulnerabilities identified.

Scope:

This policy covers all information systems within the EMCBC environment, including General Support Systems, Major Applications, and Minor Applications. All EMCBC information systems must undergo a formal risk assessment process as part of Certification and Accreditation.

Roles and Responsibilities:

Role	**Responsibilities**
AO, AODR	• Provide appropriate DOE policies, orders and guidance to ensure that the security controls are cost effective and sufficient to protect the information and information systems based on the operational risks. • Review all systems to ensure that the missions of the EMCBC are protected. • Review and approve all FIPS 199 sensitivity classifications for all EMCBC accreditation boundary systems or enclaves.
ISSM	• Develop and implement risk assessment procedures and ensure they are: o Documented; o Disseminated to appropriate persons within the organization; o Reviewed by responsible parties at least annually; and o Updated to maintain an accurate description of system operations. • Review and approve the POA&M(s).
ISSO	• Review all risk assessments to ensure the risk mitigation strategies selected are appropriate and that the system owners have developed and maintain an appropriate set of documentation.

Role	Responsibilities
System Administrator, Application/Data Owners, Line Managers	• Implement this policy, including the preparation and timely maintenance of all required documentation; • Review risk assessments annually or when a major change to the system environment occurs; and • Identify risks with an unacceptable level of mitigation and ensure, for further security controls, that they are included and tracked through resolution in the POA&M.

Compliance:

This Risk Assessment Policy Statement will be implemented through the preparation of an EMCBC Risk Assessment Policy and supported by documented procedures. The procedures shall:

- Be reviewed annually and updated to address any new risk factors;
- Be consistent with the EMCBC's mission, functions, directives, policies, regulations, standards, and guidance;
- Include categorization of the information system and the information being processed, stored, or transmitted by the system in accordance with FIPS 199 and document the results (including supporting rationale) in the system security plan;
- Address assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the laboratory;
- Ensure that risk assessments are updated annually or when there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system; and,
- Establish assessment techniques on a recurring basis to detect new vulnerabilities in the information system.

ATTACHMENT 10.2

Security Planning (PL) Policy Statement

Purpose:

The security planning policy provides guidance for developing the documentation for information or information systems as required by the Federal Information Systems Management Act (FISMA) and NIST. The system security plan (SSP) provides the basis by which the AO will assess the security controls and make a decision on the operational status that should be granted.

Scope:

This policy covers the processes and procedures that will be used by the EMCBC to develop, maintain, and update each System Security Plan (SSP). Once the SSP has been developed it must be tested to validate that the security controls designated in the Energy PCSP are operational and functioning as planned. Once that testing has been accomplished the entire package will be compiled and presented to the AO who will make an operational decision for the system or enclave.

This policy prescribes the review and update processes for the SSP when a significant change has occurred or when other operational requirements may dictate the need for reviewing the system/enclave's operational status. In addition, all EMCBC SSPs will be reviewed at least annually to ensure the protection of all computing resources that correspond to the EMCBC accreditation boundary.

Roles and Responsibilities:

Role	**Responsibilities**
AO	• Review and approve the operational status of the cyber systems in EMCBC accreditation boundary. • Make appropriate changes to the operational status based on the risk factors associated with continued operations when there is a change to the security status of the system.
AODR	• Approve the SSPs and provide the AO with an operational recommendation for the accreditation boundary.

Role	Responsibilities
ISSM	• Review each SSP for completeness and accuracy. • Provide the AODR with a recommendation relating to approval of the SSP created by the Application/Data Owner. • Independently assess the implementation of security controls for all systems/enclaves to provide assurance that the systems are being operated as documented. • Develop a standard "Rules of Behavior User Agreement" document and ensure that all personnel have read and understand their responsibilities concerning the rules of behavior. • Determine if any systems collect information that necessitates the completion of a privacy impact assessment (PIA). If any systems collect this information the PIA will be conducted and included with the SSP.
ISSO	• Collaborate with the system administrator, application/data owner and line managers to develop an application level security requirement. • Develop, document and implement the SSP for the systems. • Review the plan and document weaknesses. • Monitor the operations of systems to verify they are administered in accordance with the SSP.
System Administrator, Application/Data Owners, Line Managers	• Report any configuration change in operational status or implementation in security controls that may modify the risk factors for the system. • Report any significant change to the operational status of the system.

Compliance:

This Security Planning Policy will be implemented through a formal EMCBC procedures document and supported by detailed procedures including:

- Development and maintenance of an SSP document in accordance with the Energy PCSP.
- Development of procedures that define a significant change and the activities required when such a change is planned.
- Documentation of procedures for review and processing of an SSP to obtain approval and the appropriate authority to operate from the AO.
- Development of procedures for validating the implementation of security controls. This validation may include a variety of techniques, how the examiner verifies the control is operational (the artifact(s) that should be available) and the documentation needed to validate the control.
- Development of guidance for the use and operation of systems within the EMCBC accreditation boundary. This document (Rule of Behavior User Agreement) shall be distributed to all users and users shall acknowledge that they have read, understand, and will follow the requirements.
- Identification of data that requires the preparation of a Privacy Impact Assessment (PIA) and preparation of a PIA if required.

ATTACHMENT 10.3

System and Services Acquisition (SA) Policy Statement

Purpose:

The EMCBC will obtain systems and services that fully comply with public law and DOE's guidance. Systems and service acquisition will be based on a life-cycle total cost of ownership model that is subject to Capital Planning and Investment Control (CPIC) review.

Scope:

The Office of Information Resource Management (IRM) develops, disseminates and periodically reviews and updates a formal documentation of system and services acquisition policy that addresses the purpose, scope, roles, responsibilities, and compliance to new standards. This policy applies to all acquisitions of information systems and services by the EMCBC under the auspices of the IRM policies.

Roles and Responsibilities:

Role	**Responsibilities**
AODR	Develop, distribute and periodically review/update a formal System and Services Acquisition Policy in compliance with IRM Policy.
ISSM	Oversee acquisition policy implementation.

Compliance:

This System and Services Acquisition Policy will be implemented through the preparation of Procedures and Technical Instruction Documents. These procedures shall be:

- Reviewed annually and updated to address any new risk factors.
- Consistent with the EMCBC's mission, functions, directives, policies, regulations, standards, and guidance.
- Consistent with DOE CPIC processes for adequately and cost effectively protecting the information and information system.
- Consistent with a structured information systems development life cycle methodology that includes computer security considerations.
- Consistent with the assessment of risk. System procurements shall include devices or software necessary to ensure that the device will meet EMCBC security control specifications.
- Completed to ensure that EMCBC complies with all software usage restrictions.

System owners shall develop procedures that:

- Enforce explicit rules governing the downloading and installation of software by users.
- Ensure that third-party providers of information system services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements. The system owner and third party organization shall monitor security control compliance.
- Ensure that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel.

ATTACHMENT 10.4

Certification, Accreditation and Security Assessment (CA) Policy Statement

Purpose:

The certification and accreditation (C&A) process verifies that EMCBC's information systems meet documented security requirements and will continue to maintain them throughout the system's life cycle. The C&A process ensures that every system encompasses the minimum level of security appropriate to the information that is being stored, processed or transmitted within the C&A accreditation boundary. These common protection requirements create a common baseline for security in all EMCBC systems for each specific type. The C&A provides the EMCBC with the authority to operate (ATO) its information systems in the manner described by the SSP.

Scope:

All EMCBC information systems must undergo a C&A process prior to initial operation. Reauthorization is required every three years or when a major change is made to the system(s). EMCBC uses an accreditation boundary (a.k.a Enclave) for certification and accreditation.

The EMCBC applies NIST guidance to determine the category of risk of all computing assets in accordance with FIPS 199. Those with the same category of risk are grouped together into one accreditation boundary know as an enclave. A description of the enclave is located in the SSP. Recommended management, operational, and technical controls are applied to provide the level of security required for the information and computer resources as determined by the risk categorization. An independent group will audit these controls to determine if they provide appropriate protection and that their state of application provides the necessary protection across the enclave. Enclaves with controls applied and working will be granted an ATO by the AO.

Roles and Responsibilities:

Role	**Responsibilities**
AODR	• Ensure that all systems are reviewed. • Provide appropriate guidance to ensure that the security controls are cost effective and sufficient to protect the information and information system based on their purpose and the operational risks.
ISSM	• Define security assessment and, certification and accreditation procedures that are: o Documented; o Disseminated to appropriate elements within the organization, including the AO & AODR; o Reviewed by responsible parties at least annually; and o Updated in a timely manner to maintain an accurate description of system operations. • Ensure that all systems are maintained and operated in accordance with their ATO. • Review and approval of the Computer Security POA&M
ISSO	• Ensure that the controls selected are appropriate • Ensure that system owners have developed and maintain an appropriate set of C&A documentation.
System Administrator, Application/Data Owners, Line Managers	• Implement this policy, including the preparation and timely maintenance of all required documentation. • Ensure the system is operated within the ATO provided by the AO. • Ensure all identified deficiencies are included and tracked through resolution in the POA&M.

Compliance:

The security assessment shall address:

- Purpose, scope, roles, responsibilities, and compliance for security assessment, certification, and accreditation activities.
- Procedures that are sufficient to address all areas identified in:
  - Federal law and applicable NIST publications;
  - DOE Order 205.1B;
  - The Energy PCSP and SSP;
  - Certification and accreditation policy; and
  - All associated security assessments.
- Procedures to ensure that policies and procedures are updated periodically, especially when organizational reviews indicate updates are required.
- Processes for an assessment of the system’s security controls which are conducted at least annually.
- Development of security assessment reports to document the system’s security controls to ensure they are implemented properly, operating as intended, and providing the appropriate protection to meet the security requirements and all policies and procedures.

- Procedures for system administrator, application/data owners, and line mangers to ensure their activities are consistent with EMCBC's security assessment procedures.
- Maintenance of records or documents to demonstrate: (i) security assessments are being consistently conducted on the information system on an ongoing basis; and (ii) if anomalies or problems encountered during security assessments are being documented and the resulting information used to actively improve security assessment policy, procedures, and processes on a continuous basis.

The security certification shall ensure that:

- A certification process is defined that determines the completeness and effectiveness of each security control. This process shall validate that the security control is implemented properly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- Procedures are consistent with NIST FIPS 199, FIPS 200, Special Publication (SP) 800-53A and other publications as deemed appropriate by the system owner.
- Development of security certification documentation includes a threat and risk analysis, SSP, ST&E results, current POA&Ms, and ATO.

Plan of Action and Milestones (POA&M) shall:

- Verify that the EMCBC develops and updates an action plan for the information system which identifies and tracks to completion shortfalls within the security controls.
- Identify deficiencies noted during any assessment or audit of the security controls. All discrepancies shall be identified and tracked using EMCBC's POA&M process. For each deficiency develop a corresponding plan of action to document EMCBC's plan to correct noted deficiencies and to reduce or eliminate known vulnerabilities in the system.
- The ISSM shall report quarterly to the AO, AODR and CSPM on the progress in completing activities to correct each shortfall.

Accreditation procedures shall address:

- The AO's process for certifying each accreditation boundary and provide a written ATO in accordance with NIST SP 800-37. The AO may authorize operations of a system or enclave for up to 3 years based on the level of risk and the operational status of security controls.
- The process for the AO to revoke the ATO for an accreditation boundary based on changes in risk or actions that may place the information or information system in jeopardy.

Continuous Monitoring shall include:

- Verification that the security controls are being monitored according to defined procedures on an ongoing basis.
- Security control monitoring procedures that are consistent with NIST Special Publication 800-37.
- Maintenance of records to determine: (i) that designated security controls are assessed; (ii) changes to or

deficiencies in the operation of the security controls are analyzed for impact, documented, and reported; and (iii) adjustments are made to the information SSP and POA&Ms, as appropriate.

- Verification that EMCBC personnel with security control monitoring responsibilities understand their roles and responsibilities and conduct operations within those guidelines.
- Reporting procedures to the AO for any deficiency or shortfall that could reasonably be expected to impact the ATO or that substantially increases the risk associated with continued operations.

ATTACHMENT 10.5

Personnel Security (PS) Policy Statement

Purpose:

The EMCBC will develop, disseminate, and periodically review and update a formal, documented, personnel security policy that addresses the purpose, scope, roles, responsibilities, and compliance with the policies and requirements of OMB, DOE, and the Energy PCSP. The EMCBC will ensure that the Assistant Director of Information Resource Management (AD-IRM) has formal, documented procedures to facilitate the hiring, management and termination of personnel as well as screening for all EMCBC personnel to implement the required defense-in-depth.

Scope:

This policy applies to all EMCBC employees as well as contractors with access to EMCBC computing resources who are required to comply with this policy in accordance with the Rules of Behavior for EMCBC Computer Systems as well as HR policies. This policy covers hiring, screening, termination, transfer, and punishment of persons with access to EMCBC computing resources (as far as their actions or the actions of this policy impact on information and information systems). This policy is not intended to replace other EMCBC, DOE, or IRM personnel policies.

Roles and Responsibilities:

Role	**Responsibilities**
Director	• Implement EMCBC Personnel policies to comply with this policy as well as Federal laws, directives and guidelines for personnel security.
Assistant Director, IRM	• Ensure that personnel positions with site administration access are identified and that appropriate pre-screening is required as a condition of employment. • Ensure that personnel positions with elevated system access to PII are identified and that appropriate pre-screening is required as a condition of employment. • Establish procedures for appropriate disposition of system access rights in conjunction with personnel transfer or termination policies.
Assistant Director, Human Resources	• Establish procedures for termination and transfer of personnel, to include notification of EMCBC for appropriate disposition of information system accounts. • Establish sanction procedures for personnel failing to comply with policies or procedures, in accordance with EMCBC and DOE policy
Line Managers	• Identify positions with site administration access or elevated system access to PII and assign a level of risk to that position description. • Review risk designations in conjunction with annual performance reviews. • Screen individuals in accordance with IRM policy.

Compliance:

This Personnel Security Control policy will be implemented through the preparation of and supported by documented procedures. The procedures shall be:

- Reviewed periodically (at least annually) and updated to address any new risk factors.
- Consistent with EMCBC's mission, functions, directives, policies, regulations, standards, and guidance.
- Created to address assigning a risk designation to all positions and establish screening criteria for individuals filling those positions. The EMCBC will review each position's risk designation annually in conjunction with annual performance reviews.
- Established to address individuals requiring screening prior to access to EMCBC information and information systems.
- Created to cover termination and transfer procedures that include appropriate disposition of information system access rights, and to ensure that appropriate personnel have access to official records created by the terminated employee that are stored on organizational information systems.

ATTACHMENT 10.6

Physical and Environmental Protection (PE) Policy Statement

Purpose:

The EMCBC will provide a safe and productive environment for personnel working at the EMCBC sites. Physical access to the information and information systems will negate many of the security controls that are being implemented. For this reason it is very important that the information and information system processing areas be properly protected. This policy puts forth the requirements for protecting the EMCBC's information and information systems from physical and environmental threats.

Scope:

Physical access to the EMCBC sites is open to proper personnel. Access to individual sites is handled through Site Safeguards and Security and their functions are not included in this policy. This policy focuses on physical access to the data center and other areas that contain network infrastructure devices (e.g., routers, switches) and information technology networking devices. This policy also covers the environmental controls, e.g. fire, water, heat, humidity, etc. that are necessary for the safe operation of these areas.

For some aspects of this policy IRM relies on the site security forces for completion of those functions. In those cases, IRM responsibility is limited to the transfer of that responsibility and to validating that the function is being completed appropriately to ensure the protection of the information and information systems.

Roles and Responsibilities:

Role	Responsibilities
Compliance & Project Support, Office of Technical Support & Asset Management (OTSAM)	• Identify site security requirements for all functions required of the facility Safeguards and Security department functions.
ISSO, System Administrators	• Perform an annual review of security agreements and controls to ensure they effectively protect the information and information systems. • Develop procedures, in concert with the Safeguards and Security personnel, to limit access to protected areas to only authorized personnel. • Monitor access to the controlled areas and ensure the procedures are being followed. • Monitor the environmental controls to ensure they are operational and functioning as necessary.
Application/Data Owners, Line Managers	• Identify any system environmental or security requirements that may be unique to their systems and provide the requirements to the appropriate personnel for review.

Compliance:

This Physical and Environmental Protection Control policy will be implemented through a formal EMCBC procedures document and supported by detailed documented procedures. This includes:

- Identifying all areas needing access control and coordinating a cost effective controls procedure for each area to ensure only authorized personnel have access.
- Developing and maintaining lists of personnel with authorized access to the data center or any other designated limited access facility containing information systems.
- Designating the access approval process and the documentation or device (e.g., badges, identification cards, and smart cards) required to gain access.
- Designating officials within the organization who review and approve the access list and authorization credentials at least annually.
- Controlling all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and verifying individual access authorizations before granting access to the facilities.
- Controlling physical access to information systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible.
- Maintaining a visitor access log to facilities (except for those areas within the facilities officially designated as publicly accessible) that includes:
  - Name and organization of the person visiting;
  - Signature of the visitor;

  - Citizenship;
  - Identification verification;
  - Escort;
  - Date of access;
  - Time of entry and departure;
  - Purpose of visit; and
  - Name and organization of person visited.

- Developing procedures to monitor physical access to information systems.
- Documenting the processes for shutting down the systems including:
  - A controlled shutdown based on any function that could potentially damage the device if it was allowed to continue to operate;
  - An emergency shutdown (e.g. fire in a data center); and
  - A shutdown when systems have been transitioned to the uninterruptible power supply (UPS) when local power is no longer available.
- Documenting the procedures in the event of a fire in areas occupied by IRM. This includes data centers, telecommunication closets and any other area that contains information systems resources.
- Documenting the procedures for monitoring temperature and humidity in the data centers, including notification to service providers.
- Documenting procedures for monitoring for water leaks or other disruptions that would negatively impact the operations of the systems and devices in the data centers.
- Documenting the processes and procedures that will be followed during the receipt, transfer, or removal of any system or device from the data center. This procedure should include the verification of information contained on the information system and the potential that the computer storage media may require removal, sanitization, or destruction.

ATTACHMENT 10.7

Contingency Planning (CP) Policy Statement

Purpose:

Contingency planning is focused on identifying and categorizing information and information systems to ensure they are appropriately protected. This policy has been developed to ensure that contingency plans appropriate to the risk and potential damage are developed and tested for each enclave/system.

Scope:

This policy covers all systems/enclaves identified in each EMCBC SSP. A contingency plan will be documented to include the necessary recovery timeframes and the primary methods that will be used to recover operations for each system. A test or verification process should be included with each plan to verify that the plan is realistic and that it can be executed.

Most of the business functions performed at EMCBC use commercially available computing resources and are all completed on commercial systems. While EMCBC has no servers or systems that meet the criteria for a Continuity of Operations Plan (COOP), EMCBC does have contingency plans in place to backup, replace, and recover systems.

Roles and Responsibilities:

Role	**Responsibilities**
ISSO	• Validate the development and testing of the contingency plan.
System Administrators, Application/Data Owners, Line Managers	• Develop a contingency plan for their system(s). • Review, approve, and test the contingency plan at least annually to ensure that it is cost effective and protects the information and information system.

Compliance:

Contingency plans will be maintained for all EMCBC information systems within an accreditation boundary.

- The Contingency Plan will be coordinated as applicable with other organizations, such as IRM, to ensure inclusiveness of other related plans as required (e.g., emergency services, natural disasters, business systems recovery plans, etc.).
- Contingency Planning training will be conducted at least annually for personnel in their roles and responsibilities with respect to the EMCBC information systems.
- The plan will be tested at least annually. Actual exercise of the plan (such as a major power loss) may be substituted for an annual test, provided it is documented as such. Table top exercises may not be used as a test more than once every two years.

- IRM shall ensure alternate storage sites are maintained and the list of personnel authorized to deliver or pickup back-up tapes is current.

ATTACHMENT 10.8

Configuration Management (CM) Policy Statement

Purpose:

A configuration management program is designed to ensure that system components are installed and maintained using standards that maximize the protection for all components of the network. The purpose of this policy is to establish a baseline policy that will define the minimum application of security controls that will be used for each element type. In addition, this policy establishes guidance for devices that either will not or cannot conform to EMCBC baseline configuration management baselines.

Scope:

This policy is applicable to all devices that are part of, or connect to, the EMCBC accreditation boundary. Configuration guidelines for devices may vary between enclaves; however, any device in the EMCBC accreditation boundary must conform to EMCBC IRM's Technical Instruction Documents (TID) configuration management guidelines. Use of personal computer equipment or electronic devices in the EMCBC accreditation boundary is strictly forbidden, unless it is approved by the AD-IRM and EMCBC configuration management team.

Roles and Responsibilities:

Role	**Responsibilities**
ISSO	• Validate configuration baselines for each type of device. • Review scans and other available information to ensure that configuration guidelines are being maintained on the network. • Mediate any request for exemption from the configuration guidelines.
System Administrators	• Develop procedures to ensure each device on the network is configured, maintained and operated within EMCBC configuration guidelines. • Remove any system that fails to conform with the guidelines. • Deploy and support their systems with the appropriate configurations.
Users	• Ensure they do not remove, modify or otherwise tamper with system configurations or remove security settings.

Compliance:

Assistant Director, IRM shall:

- Develop and maintain an inventory of device types, operating systems and other critical elements necessary for defining configuration standards.
- Develop an approved configuration baseline for each device, operating system or other element to ensure each device is operating in a manner to protect the information and information systems.
- Develop procedures for ensuring each device has the baseline configuration standards implemented.
- Develop processes to rapidly identify when a system configuration has been changed and to return that system to the approved baseline configuration.
- Develop procedures for systems owned by EMCBC to be used on the EMCBC accreditation boundary. These procedures shall include ensuring that the systems are maintained and operated in a manner consistent with EMCBC policies and to ensure that they present no additional threat to the environment.
- Work with the system administrator and application/data owners to identify any system that increases the risk to the EMCBC accreditation boundary to remediate the deficiency. This authority includes the immediate removal of any system that may be conducting activities in violation of EMCBC policy, e.g. scanning or other nefarious activity.
- Conduct scans to validate and verify device configurations. Provide an automated function to return devices found to have configuration modifications back to the approved setting.

ATTACHMENT 10.9

Maintenance (MA) Policy Statement

Purpose:

The maintenance program is established to provide a standard based system for the long term support of all devices connected to the EMCBC accreditation boundary. By providing appropriate maintenance the long term reliable operations of each device can be ensured. In addition, by following the maintenance polices the security configuration of the device will be maintained.

Scope:

The maintenance policy is applicable to all EMCBC owned devices that connect to the accreditation boundary. In addition, the policy applies to devices that support the operations of IRM. Most of these devices are under the control of OTSAM at the EMCBC, however, responsibilities to ensure that these services are appropriate to the continued operation of the IRM functions do exist.

The maintenance policy also includes contracts for software and software related functions at the EMCBC. Contracts for all maintenance functions are included in this policy.

Roles and Responsibilities:

Role	**Responsibilities**
Assistant Director, IRM	• Review maintenance contracts to ensure EMCBC computer security policies are incorporated within the contract terms and conditions
System Administrators	• Develop procedures that maintain the security controls structure while allowing maintenance personnel required access; • Monitor maintenance activities with respect to computer security principles; • Track the use of maintenance contract personnel and their access to site devices; and, • Use appropriate processes to maintain the security controls for all devices during maintenance.

Compliance:

This system maintenance policy will be implemented through a formal EMCBC Procedures Document and supported by documented procedures. Procedures will:

- Be developed, disseminated, and periodically reviewed/updated to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.
- Schedule, perform, and document routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.
- Approve, control, and monitor remote and locally executed maintenance and diagnostic activities.
- Maintain a list of personnel authorized to perform maintenance on the information system. Only authorized personnel perform maintenance on the information system.
- Ensure the organization maintains a maintenance log for the information system that includes: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) citizenship; (iv) name of escort, if necessary; (v) a description of the maintenance performed; and (vi) a list of equipment removed or replaced (including identification numbers, if applicable).

ATTACHMENT 10.10

System and Information Integrity Control (SI) Policy Statement

Purpose:

EMCBC will provide a safe and secure computing environment that is free from viruses, spam, and spy ware to the maximum extent possible. The AD-IRM ensures that software patches and upgrades are applied promptly and/or consistent with the level of risk and local mission requirements and that anti-virus and malicious code threats are blocked to the maximum extent possible.

Scope:

This policy covers all devices connected to the EMCBC accreditation boundary, whether directly or remotely, including devices connected internally and those connected to the Visitor enclave. This policy covers the areas of patching, anti-virus, spy ware, malicious code, and vulnerability scanning and assessments.

Roles and Responsibilities:

Role	**Responsibilities**
Assistant Director, IRM	• Develop and implement the System and Information Integrity procedures.
ISSM	• Monitor the internet security environment through subscriptions to mailing lists and security forums to ensure that new threats are identified and countermeasures implemented as quickly as possible. • Implement processes and techniques for intrusion detection and monitoring of critical network segments and servers. • Scan for common vulnerabilities and patch levels on all accessible systems at least once per week.
ISSO, System Administrators	• Ensure all government-owned systems have anti-virus or anti-spy ware installed as part of the baseline configuration as prescribed in EMCBC Rim's TID. • Provide anti-virus updates to users at least once per week. • Implement spam filtering on email servers • Ensure all anti-virus software is updated regularly, not less than once per week. • Implement and administer patching and update procedures and ensure systems have appropriate patches and updates applied. • Identify and correct information system flaw and share information with ISSM.
Users	• Ensure that all anti-virus software is updated regularly, not less than once per week. • Ensure all systems have appropriate patches applied.

Compliance:

This System and Information Integrity Control policy will be implemented through the preparation of and supported by documented procedures. The procedures shall:

- Be reviewed periodically (at least annually) and updated to address any new risk factors.

- Be consistent with EMCBC missions, functions, directives, policies, regulations, standards, and guidance.
- Address monitoring of connected systems for compliance to include installation and updating of anti-virus software and application of critical patches.

IRM shall:

- Implement malicious code protection that includes a capability for automatic updates.
- Receive and review information system security alerts/advisories on a regular basis, issue alerts/advisories to appropriate personnel, and take appropriate actions in response.
- Employ tools and techniques to monitor events on information systems, detect attacks, and provide identification of unauthorized use of the systems.

ATTACHMENT 10.11

Media Protection Control (MP) Policy Statement

Purpose:

EMCBC will enforce activities to safeguard physical media and the information on that media from unauthorized disclosure.

Scope:

This policy applies to the transfer, disposal, or any other activity that may result in the unauthorized release of information. This policy applies to all information produced, stored, processed, or otherwise contained within any device that connects to the EMCBC accreditation boundary. This policy also covers printed matter that is generated from information contained or processed on an EMCBC information system.

This includes personally identifiable information (PII) and other information that the data owner deems as needing additional controls. This policy covers those systems and ensures that the media is appropriately protected when transferred or removed.

Roles and Responsibilities:

Role	**Responsibilities**
ISSM	• Review media protection procedures to validate that they appropriately protect EMCBC information. • Develop procedures for the sanitization or destruction of computer storage devices to ensure the protection of all EMCBC information types. • Monitor the procedures to ensure they are being applied appropriately.
Application/Data System Owners, Line Managers	• Identify the type of information stored on each system.
System Administrators	• Follow EMCBC policy when transferring or excessing any system or device and validate the device has been properly sanitized.

Compliance:

This Media Protection Control policy will be implemented through a formal EMCBC Procedures Document and be supported by documented procedures. Documentation will consist of:

- Ensuring unauthorized users do not have access to information in printed form or on digital media removed from information systems.

- A process that sanitizes or destroys information system digital media before its disposal or release for reuse outside the organization, to prevent unauthorized individuals from gaining access to and using the information contained on the media. (note: physical destruction is preferred for any device leaving EMCBC)

- Requiring external labels on removable computer storage media and information system output indicating the distribution limitations and handling caveats of the information, based on a risk assessment of the information. Routine labeling of encrypted information is not applicable.
- Requiring physical controls and secure storage of information system media based on the highest FIPS 199 security category of the information recorded on the media.
- Requiring controls for information system media that restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel.
- Requiring sanitization of information system digital media using approved equipment, techniques, and procedures.

ATTACHMENT 10.12

Incident Response Control (IR) Policy Statement

Purpose:

Incident response controls provide those security controls that protect EMCBC's information and information systems by properly responding to security incidents. This policy defines the roles and responsibilities for individuals and organizations that may be involved in an incident. This policy also provides direction for assessing and reporting on that incident to allow others to rapidly identify and correct a similar incident.

Scope:

This policy covers all EMCBC information and information systems. This includes all networks and devices that may connect to the EMCBC accreditation boundary. EMCBC has the responsibility to put in place policies and procedures that include identifying, controlling, eliminating, investigating, and reporting on all computer security related incidents.

Roles and Responsibilities:

Role	**Responsibilities**
ISSM	• Review incident reports to validate their completeness and assess the need for updates to policies or procedures. • Forward incident reports in accordance with the Energy PCSP. • Develop an incident response program and identify an incident response team in writing.
ISSO	• Validate that the vulnerabilities identified as part of an incident have been removed or mitigated.
System Administrators and Users	• Identify potential incidents and report incidents to the computer security group.
Incident Response Team	• Maintain expertise to handle all types of information security incidents. • Identify, correct, track and document each incident. • Support application/data owners and system administrators during recovery of the incident. • Track the incident through conclusion and complete applicable reports.

Compliance:

This Incident Response Control policy will be implemented through a formal EMCBC Procedures Document/Manual. The incident response procedures shall:

- Validate that EMCBC follows DOE and EM requirements for incident response (DOE O 205.1B) and the Energy PCSP.

- Implement an incident handling capability for security incidents that include preparation, detection and analysis, containment, eradication, recovery, and follow-up.
- Define the steps to be taken, and by whom, when a computer attack poses a major threat.
- Document training requirements for personnel in their incident response roles and responsibilities. This shall include annual refresher training.
- Define incident response testing and exercises, and document those used to determine incident response program effectiveness.
- Track and document computer security incidents on an ongoing basis.
- Employ mechanisms to increase the availability of incident response information and support.

ATTACHMENT 10.13

Awareness and Training (AT) Policy Statement

Purpose:

To ensure that personnel receive information and skills appropriate to their system access rights (e.g. users, administrators, domain administrators, and computer security professionals) to properly use and protect the information and information systems which they have access and that all personnel are aware of their responsibilities under *EMCBC's Computer Security policies and procedures.*

Scope:

This policy is applicable to all users granted access to EMCBC resources, whether directly or remotely. All users must undergo basic security awareness training prior to being granted access to EMCBC information systems resources. At a minimum, basic awareness training must incorporate acceptable use of resources, basic security procedures (such as password choice), and incident reporting procedures.

Roles and Responsibilities:

Role	**Responsibilities**
ISSM	• Develop and implement the EMCBC Computer Security Training Program • Ensure training material is current, relevant and appropriate to the EMCBC personnel
Director, Human Resources	• Ensure new employees take the Computer Security Awareness Training when first logging on to the EMCBC network.
ISSO, System Owners, Line Managers	• Ensure personnel comply with this policy.
Users	• Complete required computer security training, including both basic and annual refresher training.

Compliance:

As a minimum, training requirements shall:

- Be reviewed at least annually and updated to address any new risk factors.
- Be consistent with the EMCBC's mission, functions, directives, policies, regulations, standards, and guidance.
- Ensure all users (including managers and senior staff) are exposed to basic information system security awareness before they are allowed access to the system.
- Provide refresher training for all personnel at least annually.
- Include identification of personnel with elevated system privileges and responsibilities, document those privileges and responsibilities, and provide appropriate information system security training before authorizing access to the system and at least annually thereafter.

- Include documentation and monitoring of individual information system security training activities, including basic security awareness training and specific information system security training, to ensure compliance with this policy.

ATTACHMENT 10.14

Identification and Authentication (IA) Policy Statement

Purpose:

To implement an identification and authentication process such that all users of EMCBC Information systems are appropriately identified and authenticated. Authentication services verify an individual's authorization to receive information or validate the authenticity of a transmission. This policy will establish authentication services that appropriately protect the information and information systems within each accreditation boundary.

Scope:

This policy applies to all personnel that use EMCBC information or information systems resources. This policy applies to any device that connects to the EMCBC accreditation boundary.

Roles and Responsibilities:

Role	**Responsibilities**
ISSM	• Review the identification and authentication processes at least annually to determine that the policy effectively protects EMCBC's information and information systems.
ISSO	• Develop procedures to effectively implement the identification and authentication policy. • Routinely monitor identification and authentication procedures to validate that all device and individual usage is monitored in accordance with this policy.
Application/Data Owners	• Implement identification and authentication processes.
System Administrators	• Implement and support all identification and authentication processes for their systems. • Report any attempt to bypass or circumvent identification and authentication processes to the ISSO and/or ISSM.
Users	• Comply with authentication and identification procedures.

Compliance:

This identification and authentication policy will be implemented through an *EMCBC Implementing Procedure* defining full compliance. This procedure will include requirements addressing every user of an EMCBC information system. The procedures shall be:

- Reviewed at least annually and updated to address any new risk factors.

- Consistent with the EMCBC's mission, functions, directives, policies, regulations, standards, and guidance.
- Inclusive of all users of the EMCBC network and services and define the identification and authentication processes for each class of user or administrator based on risk to EMCBC's information resources.
- Designed and established to ensure that individuals are accountable for their actions and that anyone abusing the services can be rapidly identified and isolated. Group and shared credentials are not routinely authorized. Anyone abusing this policy shall have their credentials removed immediately and be forwarded for administrative action.
- Developed to reasonably allow personnel access to services based on their need and the risk they present to EMCBC.
- Established to ensure all personnel understand their responsibilities and limitations and require a signature, including electronic signatures, to these limitations.
- Established to limit the ability of users to continually attempt to access a system. This includes locking systems after a limited number of unsuccessful login attempts or continuous monitoring or alerts when these types of activities are attempted.
- Developed to ensure that approved protocols do not allow the use of reusable passwords or credentials be transmitted in the clear.

ATTACHMENT 10.15

Access Control (AC) Policy Statement

Purpose:

The purpose of the access control policy is to ensure that access to systems is provided only to authorized users and devices. Access controls provide those security controls that protect the EMCBC information systems by properly authenticating the user/device before providing access to the information or information system.

This policy defines the procedures that are required to support access control. This includes the requirement for validation of the access requirement, completion of security awareness training, agreement to work within EMCBC policy, and validation of the individual's identity when credentials are issued.

Application/data owners as well as system administrators are responsible for establishing procedures for granting, maintaining, and removing access from information systems, applications, and resources.

Scope:

The DOE and EMCBC provide staff with the computing resources needed to support official government business. Access to EMCBC resources is a privilege granted based on the needs of DOE, EMCBC, and the user. Each person with authorized access to EMCBC computing resources must agree to comply with all applicable policies and regulations.

This policy grants access to foreign nationals under limited circumstances. Specific requirements for granting access to foreign nationals will be developed if needed.

This policy includes all users requiring access to EMCBC's information systems inclusive of whether functions are performed locally or through remote access.

Guests utilizing guest networks are not subject to this policy. Access to the guest network will be controlled by the visitor's sponsor and such access may include foreign nationals. The guest network is isolated from all contact with the rest of the accreditation boundary and is provided for individuals needing access to their home networks. Procedures for guest networks will be reviewed annually.

Roles and Responsibilities:

Role	**Responsibilities**
Assistant Director, IRM	• Implement and administer Access Control Policy.
ISSO	• Verify and validate that only approved individuals have access to EMCBC information and information systems.
System Administrators, Line Managers	• Establish and maintain procedures for access control of users and systems.
Application/ Data Owners, Line Managers	• Ensure only personnel with a valid requirement are provided access, access is removed when the need no longer exists, and any violation of access is immediately reported to the ISSO.
Users	• Complete required actions and comply with EMCBC access control policies.

Compliance:

This Access Control policy will be implemented through EMCBC Procedures Document/Manual defining full compliance. Procedures shall:

- Be reviewed at least annually and updated to address any new risk factors.
- Be consistent with the EMCBC's mission, functions, directives, policies, regulations, standards, and guidance.
- Be developed to ensure personnel are assigned, and given both the responsibility and authority, to ensure that access is granted on a need basis and when that need no longer exists the access is removed.
- Be consistent with the needs of the application/data system owner, user, and EMCBC. These procedures shall be consistent with the level of risk that has been accepted by the AO in the C&A process.
- Include periodic review of access control lists and the removal or suspension of accounts that are no longer required for near term access.
- Train all authorized EMCBC personnel, with access control responsibilities, to ensure they document and report any anomalies or problems discovered within their systems. Anomalies shall be reported in accordance with the incident reporting procedures.
- Define reasonable use of the computer resources (including limited personal use). This should be reflective of The Rules of Behavior for EMCBC Computer System document, which outlines the criteria for reasonable use, limited personal use, and inappropriate use.

ATTACHMENT 10.16

Audit and Accountability (AU) Policy Statement

Purpose:

To ensure that all appropriate information is collected on the actions of devices and users to allow for efficient system management and to assist in the identification and investigation of potential security incidents.

Scope:

This policy applies to all persons and devices that operate on the EMCBC network. The precise auditing and other functions that will be used to ensure accountability are dependent on the operating system capability. This policy is established to provide the information that may be required to investigate an incident or to analyze the activities of a specific user. This policy includes retention periods for audit information.

Roles and Responsibilities:

Role	**Responsibilities**
ISSO	• Ensure that audit logs are reviewed and actions are taken to address anomalies or potential issues. • Review of the activities being logged and ensure that they are sufficient to investigate potential events.
System Administrators	• Develop procedures to review and respond to information provided from audit log reviews. • Ensure that systems have auditing activated and that audit logs are reviewed in a timely manner. • Provide access to central log servers for the maintenance and archival of system logs. • Provide log parsing and reduction tools. • Enable and maintain auditing on all systems in accordance with the guidance in the SSP. • Review logs on a daily basis for security events and reporting of suspected security events.
Users	• Do not remove, modify or otherwise tamper with audit logs or log settings.

Compliance:

The AD-IRM shall perform audits as identified in the list of auditable events specified in the Energy PCSP and SSP. These auditable events will be generated and log reports produced in the timeframes specified by the AD-IRM. Audit procedures shall ensure:

- Appropriate data is captured providing traceability back to the event occurrence and the event outcome.

- Auditable events are stored for an appropriate time period as defined by this policy, the Energy PCSP, SSP, DOE policy, or by IRM. The period shall be sufficient to provide the necessary information for incident investigations.
- The information system provides the capability to include detailed information in the audit records for audit events identified by user, time, type, location, and activity.
- Logs are regularly reviewed for inappropriate or unusual activity. Activity is investigated, reported, and action taken.
- All networked systems must provide consistent time stamps using a network time synchronization function for audit records.

ATTACHMENT 10.17

System and Communications Protection (SC) Policy Statement

Purpose:

The EMCBC will implement system and communications protection security controls consistent with the accreditation boundaries and a defense-in-depth, segmentation, and isolation strategy consistent with the risk mitigation strategy.

Scope:

This policy covers all devices authorized for use in the EMCBC accreditation boundary. This policy covers the areas of network segmentation, boundary protection, transmission integrity and all other components of the protection and transmission of information.

Roles and Responsibilities:

Role	**Responsibilities**
Assistant Director, IRM	• Ensure appropriate resources (including hardware, software, and personnel) are available to implement the network security architecture.
ISSM, ISSO	• Develop and implement a network security architecture that meets the requirements of this policy. • Review changes to the network architecture design for security compliance. • Implement monitoring solutions to detect attacks on the network. • Validate the system and communications procedures effectively protect the information and information systems.
System Administrators	• Ensure network devices and hosts are configured in accordance with baseline security standards to facilitate prevention and early detection of attacks.

Compliance:

This System and Communications Protection policy will be implemented through the preparation of EMCBC *System and Communications Protection procedures.* The System and Communications Protection procedures shall:

- Be reviewed annually and updated to address any new risk factors.
- Be consistent with EMCBC's missions, functions, directives, policies, regulations, standards, and guidance.
- Include monitoring and controlling communications at the external boundary of the information system and at key internal boundaries within the accreditation boundary. The architecture shall

provide a means of isolating a group of devices or an enclave to limit security incidents.

- Address the issue of denial of service attacks and how the architecture will address this activity.
- Prioritize the information systems to facilitate a return to service in the event of a situation that will require restarting all or a major number of systems.
- Ensure that information is transmitted in a manner that will validate the integrity of the transmission and limit the potential of data being modified in transit.
- Address the generation, distribution or use of mobile code (java, ActiveX controls, or applets) in applications used or developed at EMCBC.
- Address the use of voice over IP or voice over data technologies.
- Assess the risk and include detailed procedures for inter-connecting the EMCBC information and information systems as part of a collaborative computing environment.
- Define and address the use of cryptography at EMCBC. Use of cryptographic devices shall be consistent with DOE orders and guidance as well as NIST standards including FIPS 140-2.
- Address publicly accessible system components (e.g., public web servers)

ATTACHMENT 10.18

Software Quality Assurance (SQ) Policy Statement

Purpose:

The EMCBC has adopted the EM Quality Assurance Program (QAP) and has issued PL-414-01, Quality Assurance Implementation Plan (QIP) in accordance with the EM QAP. The EM QAP requires the use of NQA-1, Quality Assurance Requirements for Nuclear Facility Applications, allowing for grading based on the importance to safety and applicability to the EMCBC mission. NQA-1, Subpart 2.7 addresses Software Quality Assurance for Nuclear and Safety Based software. The EMCBC QIP requires a graded utilization of these standards for non-Nuclear, non-Safety based software. This policy describes EMCBC's approach to meeting these requirements.

Scope:

This policy is applicable to all software, in-house developed or acquired, utilized within the EMCBC boundary.

Approach:

The EMCBC takes an integrated approach to Cyber Security and Software Quality Assurance.

The EMCBC Authority to Operate is based on implementation of a System Security Plan (SSP), meeting the requirements of DOE O 205.1B and the associated Energy PCSP. The SSP includes Boundary and Characterization sections which bound the type of information and business systems that the system is authorized to manage. EMCBC leverages the boundary descriptions and characterization sections of the SSP to effectively grade out some software applications. The current and foreseeable future characterization of EMCBC systems, based on the EMCBC mission, effectively grades all software applications managed by EMCBC below the level of Nuclear Safety and Safety Based software. Additional grading is done within the Information Management Procedure based on the type of information being handled and completion of a software quality checklist. The following tables summarize grading of software applications at EMCBC.

TABLE 1
CHECKLISTS FOR SOFTWARE CLASSIFICATION DETERMINATION

PART A: Checklist for Nuclear Safety-Impacting Software

Software Title(s):____

Software Owner:________________________ **Project/Program Information Officer**______________________________

Check as applies:

1. _____New Software _____Existing Software

2. _____Off-the-Shelf _____Spreadsheet/Database Report

_____Custom, Vendor _____Custom, In-house _____Process Control

This checklist determines if the software being assessed impacts nuclear safety, using these definitions:

Nuclear Safety: Prevention of radiological harm to workers, the public, or the environment from nuclear activities.
Nuclear Activities: Activities with the potential to cause radiological harm from ionizing radiation.

NUCLEAR SAFETY-IMPACTING SOFTWARE CHECKLIST

NO.	QUESTION	YES	NO
1	Does the software ONLY support objectives in one or more of the following functional areas? Technology Programs (TP) Financial Management (FM) Project Control (PC) Public Involvement (PI) Human Resources (HR) Property Management (PM)		

	IF THE ANSWER TO QUESTION 1 IS "YES," THE SOFTWARE IS NOT NUCLEAR SAFETY-IMPACTING. DO NOT COMPLETE THE REMAINDER OF PART A. CONTINUE WITH PART B OF THIS FORM.
	IF THE ANSWER TO QUESTION 1 IS "NO," CONTINUE WITH PART A.		

2	Does this software produce data used to determine personnel access to radiological areas?		
3	Is the software used to detect or measure radioactivity, or does it support the management and control of radiological areas including posting?		
4	Does this software perform tracking or accountability for Enriched Restricted Material (ERM)?		
5	Is this software used to determine ERM physical storage dimensions/arrays?		
6	Does this software determine or monitor personnel, facility, or environmental radiation exposure or contamination (e.g., release, radiation work limits, dose rates)?		
7	Is this software used to measure or test facility, component, equipment, or container conformance for nuclear material to an established requirement (e.g., performance grading, quality level, or specification)?		
8	Does this software determine or implement emergency actions related to nuclear safety?		
9	Is this software necessary to develop a safety basis requirement (SBR) or technical safety requirement (TSR)?		
10	Does this software determine or control operational limits, settings, status, or equipment configurations (e.g., flows, temperatures, positions, process logic controls, human machine interfaces, operational parameters) established or described in safety basis documentation (SBD)?		

	IF THE ANSWER TO ANY OF QUESTIONS 2 THROUGH 10 IS "YES," CHECK THE "YES" BOX BELOW. THE SOFTWARE IS NUCLEAR SAFETY-IMPACTING. DO NOT COMPLETE PART B OF THIS FORM. CONTINUE WITH PART C OF THIS FORM.
	IF THE ANSWER TO ALL OF QUESTIONS 2 THROUGH 10 IS "NO," CHECK THE "NO" BOX BELOW. THE SOFTWARE IS NOT NUCLEAR SAFETY-IMPACTING. CONTINUE WITH PART B OF THIS FORM.		

RESULT: IS THE SOFTWARE NUCLEAR SAFETY-IMPACTING? □ YES □ NO

PART B: Checklist for Mission/Business-Essential Software

This checklist determines if the software is Mission/Business-essential, Select, or Other Managed software, using these definitions:

Mission-Essential: Supports an activity/process that is necessary for successful achievement of the site's mission.
Business-Essential: Supports a core business activity or process.
Select: Not Nuclear Safety-Impacting or Mission/Business-Essential but still requires control.
Other Managed: Software used for display of informational data only.

MISSION/BUSINESS-ESSENTIAL, SELECT, OTHER MANAGED SOFTWARE CHECKLIST			
NO.	**QUESTION**	**YES**	**NO**
1	Is this software used for the display of informational data only?		

IF THE ANSWER TO QUESTION 1 IS "YES," THE SOFTWARE IS OTHER MANAGED. DO NOT COMPLETE THE REMAINDER OF PART B. CONTINUE WITH PART C OF THIS FORM.
IF THE ANSWER TO QUESTION 1 IS "NO," CONTINUE WITH PART B.			

2	Is this software used to engineer, analyze, or calculate facility equipment designs, and/or configurations?		
3	Will the loss of irreplaceable or difficult-to-construct data (e.g., tests, samples, etc.) cause an unacceptable break in the continuity of operation for the user or owner organization?		
4	Is this software used to determine or select remedial actions for environmental cleanup of contaminated sites or facilities?		
5	Is this software used to evaluate present or future hazards from an implemented or proposed remedial action?		
6	Is this software used to protect facilities from inside or outside threats (e.g., facility security, fire protection)?		
7	Will a software-processing error or failure require more than $100K to resolve?		
8	Does this software determine or implement emergency actions other than nuclear-related?		
9	Would a processing error or failure of the software have a legal impact or external milestone impact?		
10	Will this software take more than 8 man-months of effort to develop, or cost more than $50K to procure or change?		
11	Is this software required to comply with state and federal regulations?		
12	Does the system/application process sensitive information?		
13	Is this software used to track procurement or contractual actions, including credit card purchases?		
14	Is this software used to provide budgets and budget components necessary to make sound business decisions?		
15	Is this software used to perform employee-related duties such as payroll or benefits?		
16	Is this software used to track government-furnished property?		
17	Is this software integral to the financial management of the project?		

IF THE ANSWER TO ANY OF QUESTIONS 2 THROUGH 17 IS "YES," CHECK THE "YES" BOX BELOW. THE SOFTWARE IS MISSION/BUSINESS-ESSENTIAL. CONTINUE WITH PART C OF THIS FORM.
IF THE ANSWER TO ALL OF QUESTIONS 2 THROUGH 17 IS "NO" CHECK THE "NO" BOX BELOW. THE SOFTWARE IS SELECT SOFTWARE. CONTINUE WITH PART C OF THIS FORM.			

RESULT: IS THE SOFTWARE MISSION/BUSINESS-ESSENTIAL? □ **YES** □ **NO**

IF NO, SOFTWARE IS SELECT SOFTWARE

PART C: Complete for All Software

1. Name of the vendor who provided the existing software or who will provide the new software (if applicable).

2. If new, is this software an upgrade to an application currently used at the EMCBC? If so, name the application.

3. Describe the purpose of the software.

4. Describe the technical requirements of the software. For example, is it standalone or LAN-based? Are current network communications adequate? If new, what is the impact on other software and systems? If new, what are the hardware requirements (memory, printers, monitors, etc.)? Not required for subcontractor.

5. What organizations use or will be affected by this software?

6. List the names of the key users or subject matter experts. Individual names not required for subcontractor.

7. Who supports, or will support, this software (for example, installation, testing, maintenance, license updates, upgrades, user support)? Information Management? Software Owner? Vendor? If more than one, explain the division of the responsibilities.

8. Identify those who are authorized to approve and accept the software before initial implementation and before changes are implemented. Individual names not required for subcontractor.

Project/Program Software Owner (print/sign):	Date:
Project/Program Information Officer (print/sign):	Date:
Manager, Information Management (print/sign): (if required by IMP-8308-05)	Date:

TABLE 2

SOFTWARE EVALUATION

Software Name:

1. What is the software classification determination?

_____Nuclear Safety-Impacting _____Mission/Business-Critical _____Select Software ____Other Managed Software

2. Has a Software Documentation Folder been created and is it being maintained as a record?

_____Yes _____No Enter file code: ______________

The following questions serve as a self-assessment to ensure all major elements of Software Quality Assurance commensurate with the software classification determination have been addressed. Attach additional documents as needed or make reference to the Software Documentation Folder.

3. Was testing documentation consistent with requirements of IMP-8308-05, Attachment 2, Contents of the Software Documentation Folder, and with IMP-8308-05, Attachment 4, Software Testing Requirements?

4. Identify individuals acting as independent reviewers or acceptance testers. (Individual names not required for subcontractor software.)

5. Describe the Software Configuration Management Plan (or make reference to the procedure). Is the plan consistent with requirements of IMP-8308-05, Attachment 3, Software Configuration Management Plan?

6. Are the source code and data security sufficient to avoid inadvertent loss (for example, not on open group drive, password-protected, etc.)?

7. Does sufficient documentation exist for use and management of the system so that another person with proper subject matter knowledge could use and support the system?

8. Overall assessment: Were the appropriate documentation, test documentation, and change control elements applied commensurate with the software classification level?

Project/Program Software Owner (print/sign):	Date:
Project/Program Information Officer (print/sign):	Date:
Manager, Information Management (print/sign): (not required for Select or Other Managed Software)	Date:

EMCBC RECORD OF REVISION

DOCUMENT TITLE:

If there are changes to the controlled document, the revision number increases by one. Indicate changes by one of the following:

l Placing a vertical black line in the margin adjacent to sentence or paragraph that was revised.

l Placing the words GENERAL REVISION at the beginning of the text.

Rev. No.	Description of Changes	Revision on Pages	Date
1	Initial Policy	All	8/27/07
2	Required Review	All	04/30/12
2	Updated to reflect Energy PCSP Revision 2.0	All	
2	Change “Site” to “Security” in titles of Sections 5.8 and 6.4	4, 9	
2	Defined acronyms	2, 8, 9	
2	Updated definition for Authority to Operate Section 5.16	5	
2	Added “The System Administrator is responsible for complying with the following program requirements:” to Section 6.8	12	
2	Changed “User Agreement Form” to “Rules of Behavior for EMCBC Computer Systems” Sections 6.10 and 9.0	14	
2	Added Section 8.1.1	14	
2	Grammatical and Formatting Corrections	All	
2	Added Software Quality Assurance Checklists	56 - 59	
2	Updated 1.0 Purpose	2	8/29/12
2	Updated 4.2 References to reflect references listed in document	2	
2	Changed Site Manager to Director on Attachment 10.5	26	
2	Changed Office of Logistics to Office of Technical Support and Asset Management	29	
2	Removed “Control” from titles of Attachment 10.10, 10.11 and 10.12	37, 39, 41	
2	Clarified process for prohibiting access to foreign nationals in Attachment 10.15	47	